

BEST AVAILABLE COPY

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-122861
 (43)Date of publication of application : 28.04.2000

(51)Int.Cl. G06F 9/06
 G06F 12/14
 G09C 1/00
 H04L 9/10
 H04L 9/34

(21)Application number : 10-297081
 (22)Date of filing : 19.10.1998

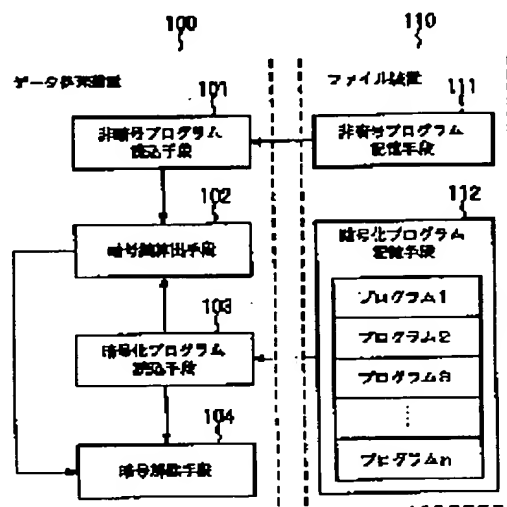
(71)Applicant : NEC CORP
 (72)Inventor : MORISHITA TAKUYA

(54) ILLEGAL ALTERATION PREVENTION SYSTEM FOR DATA OR THE LIKE AND ENCIPHERING DEVICE USED WITH THE SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a technique that prevents an illegal user from altering software and data and illegally attempting to use them.

SOLUTION: An encipher program storing means 112 stores enciphered program codes while being divided into plural blocks. A cryptographic key calculating means 102 uses a one-way function (hash function, etc.), of a program code currently existing on a main storage and calculates a cryptographic key for performing cipher release of an enciphered program code stored in the means 112 to be next executed. When the program code is partially altered to illegally use software, a correct cryptographic key can not be obtained and the execution of the program stops.



LEGAL STATUS

[Date of request for examination] 19.10.1998
 [Date of sending the examiner's decision of rejection]
 [Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
 [Date of final disposal for application]
 [Patent number]
 [Date of registration]
 [Number of appeal against examiner's decision of rejection]
 [Date of requesting appeal against examiner's decision of rejection]
 [Date of extinction of right]

Copyright (C); 1998,2000 Japanese Patent Office

THIS PAGE BLANK (USPTO)

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開2000-122861

(P2000-122861A)

(43)公開日 平成12年4月28日(2000.4.28)

(51)Int.Cl. ⁷	識別記号	F I	テマコト(参考)
G 0 6 F 9/06	5 5 0	G 0 6 F 9/06	5 5 0 B 5 B 0 1 7
12/14	3 2 0	12/14	3 2 0 B 5 B 0 7 6
G 0 9 C 1/00	6 6 0	G 0 9 C 1/00	6 6 0 D 5 J 1 0 4
H 0 4 L 9/10		H 0 4 L 9/00	6 2 1 Z
9/34			6 8 1

審査請求 有 請求項の数 6 O L (全 6 頁)

(21)出願番号 特願平10-297081

(22)出願日 平成10年10月19日(1998.10.19)

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72)発明者 森下 卓也

東京都港区芝五丁目7番1号 日本電気株式会社内

(74)代理人 100082935

弁理士 京本 直樹 (外2名)

Fターム(参考) 5B017 AA06 AA07 BA07 BB03 CA15
CA16

5B076 AB09 AB10 FA13

5J104 AA12 EA25 NA11 NA12 NA27

NA37 PA14

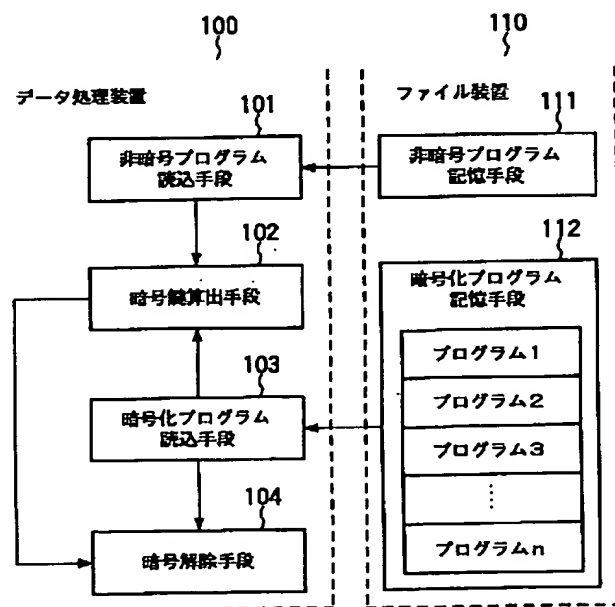
(54)【発明の名称】 データ等の不正改竄防止システム及びそれと併用される

暗号化装置

(57)【要約】

【課題】不正利用者がソフトウェアやデータを改竄し、不正利用する試みを防止できる技術を提供する。

【解決手段】暗号化プログラム記憶手段112には暗号化されたプログラムコードが複数のブロックに分割されて格納されている。暗号鍵算出手段102は現在主記憶上にあるプログラムコードの一方関数(ハッシュ関数等)を使用し、暗号化プログラム記憶手段112に格納されている次に実行するブロックの暗号化されたプログラムコードを暗号解除するための暗号鍵を算出する。ソフトウェアを不正利用するためにプログラムコードの一部を改竄すると正しい暗号鍵が得られず、プログラムの実行が停止する。



【特許請求の範囲】

【請求項1】データ処理装置とファイル装置とで構成されるデータ等の不正改竄防止システムであり、前記ファイル装置は、データの先頭ブロックを格納する第1の記憶領域と、この先頭ブロックに後続する n 個のブロックを格納する第2の記憶領域から構成され、前記 n 個のブロックの中の1番目のブロックは、前記第1の記憶領域のデータに基づいて生成された第1番目の暗号鍵で暗号化されて格納され、前記 n 個のブロックの中の i ($2 \leq i \leq n$) 番目のブロックは、 $(i-1)$ 番目のブロックのデータに基づいて生成された第 i 番目の暗号鍵で暗号化されて格納され、前記データ処理装置は、前記第1の記憶領域のデータを読み出す第1の読出手段と、前記第2の記憶領域のデータを読み出す第2の読出手段と、前記第2の読出手段により読み出された i 番目のブロックを、供給される i 番目の暗号鍵を用いて暗号解除する暗号解除手段と、前記第1の読出手段の出力に基づいて、前記第1番目の暗号鍵を生成し、前記暗号解除手段に供給するとともに、前記暗号解除手段からの $(i-1)$ 番目のブロックの暗号解除出力に基づいて、前記第 i 番目の暗号鍵を生成し、前記暗号解除手段に供給する暗号鍵算出手段とから構成されるデータ等の不正改竄防止システム。

【請求項2】前記データは、プログラムコードであることを特徴とする請求項1に記載のデータ等の不正改竄防止システム。

【請求項3】前記第1の記憶領域には、データの先頭ブロックが前もって定められた第0番目の暗号鍵によって暗号化されて格納されており、前記第1の読出手段は、この第0番目の暗号鍵により前記第1の記憶領域格納データを暗号解除して出力することを特徴とする請求項1、2に記載のデータ等の不正改竄防止システム。

【請求項4】前記暗号鍵算出手段は、1方向関数を用いて、前記第1から第 n の暗号キーを生成することを特徴とする請求項1、2または3に記載のデータ等の不正改竄防止システム。

【請求項5】データを第1から第 $(n+1)$ 番目のブロックに分割する手段と、前記第1から第 n 番目のブロックのデータに基づいて、第1から第 n の暗号鍵を生成する手段と、前記第1から第 n の暗号鍵に基づいて前記第2から第 $(n+1)$ 番目のブロックをそれぞれ暗号化する暗号化手段と、前記第1番目のブロックと暗号化された第2から第 $(n+1)$ 番目のブロックを出力する出力手段とから構成される暗号化装置。

【請求項6】前記出力手段は、前記第1番目のブロック

を前もって定められた第0番目の暗号鍵で暗号化して出力することを特徴とする請求項5に記載の暗号化装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、コンピュータソフトウェアやデータを、不正利用者が改竄し、これらソフトウェアやデータを不正利用（不正コピー等）する試みを防止できる技術に関わる。

【0002】

【従来の技術】コンピュータソフトウェアの不正コピーを防止するための手法としては、例えば特開平9-231137「複製判定方法および読出装置」に記載のものが知られている。この従来例では特定の誤り率 K を含むキー・コードをCD-ROMの一部に記録している。この誤り率 K は、CD-ROMの読み出し装置に設けられている誤り訂正符号化復号化装置では、完全には訂正が不可能な値に定められている。不正にCD-ROMを複製した場合、このキー・コードの誤り率が変化する。この従来技術では、この現象を利用して、搭載されたCD-ROMが不正に複製されたCD-ROMか否かを判定し、複製されたCD-ROMと判定された場合には、読み出し装置が動作しないように構成されている。

【0003】また、同種の不正コピー防止技術として、特定のキーを持つ簡易なハードウェアをシステムに付加し、プログラムの実行時にこのキーの値が正規の物かを判定して正規の値の場合のみ実行を許可するシステムが広く知られている。

【0004】

【発明が解決しようとする課題】しかし、これらの従来技術には、次のような問題点があった。

【0005】第1の問題点は、プログラムコードを解析し、どういった機構で不正コピーを判定しているかを調査することが容易なことである。その理由は、プログラムコードを逆アセンブラツールなどの解析ツールで解析し、その解析結果に基づいて、そのプログラムを改竄することにより、不正利用が可能となるためである。

【0006】第2の問題点は、プログラムコードを改竄されるとコピー媒体での実行を防げることができないことである。その理由は、コピー媒体の判定を行っている部分のプログラムコードを、コピーされた媒体を検出しても、常にオリジナルな媒体と判定するように改竄された場合、コピー媒体でそのソフトウェアを実行されることを防ぐことはできないためである。同様の問題は、プログラムに限らず、一般のデータでも起こりうる。

【0007】

【課題を解決するための手段】本発明のデータ等の不正改竄防止システムは、データ処理装置とファイル装置とで構成されるデータ等の不正改竄防止システムであり、前記ファイル装置は、データの先頭ブロックを格納する第1の記憶領域と、この先頭ブロックに後続する n 個の

ブロックを格納する第2の記憶領域から構成され、前記n個のブロックの中の1番目のブロックは、前記第1の記憶領域のデータに基づいて生成された第1番目の暗号鍵で暗号化されて格納され、前記n個のブロックの中の i ($2 \leq i \leq n$) 番目のブロックは、 $(i-1)$ 番目のブロックのデータに基づいて生成された第 i 番目の暗号鍵で暗号化されて格納され、前記データ処理装置は、前記第1の記憶領域のデータを読み出す第1の読出手段と；前記第2の記憶領域のデータを読み出す第2の読出手段と；前記第2の読出手段により読み出された i 番目のブロックを、供給される i 番目の暗号鍵を用いて暗号解除する暗号解除手段と；前記第1の読出手段の出力に基づいて、前記第1番目の暗号鍵を生成し、前記暗号解除手段に供給するとともに、前記暗号解除手段からの $(i-1)$ 番目のブロックの暗号解除出力に基づいて、前記第 i 番目の暗号鍵を生成し、前記暗号解除手段に供給する暗号鍵算出手段；とから構成される。

【0008】また、本発明の暗号化装置は、データを第1から第 $(n+1)$ 番目のブロックに分割する手段と；第1から第 n 番目のブロックのデータに基づいて、第1から第 n の暗号鍵を生成する手段と；前記第1から第 n の暗号鍵に基づいて前記第2から第 $(n+1)$ 番目のブロックをそれぞれ暗号化する暗号化手段と；前記第1番目のブロックと暗号化された第2から第 $(n+1)$ 番目のブロックを出力する出力手段；とから構成される。

【0009】

【発明の実施の形態】図1を参照すると、本発明のソフトウェアの不正利用防止システムの一実施形態は、プログラム制御により動作するデータ処理装置100と、ファイル装置110とから構成されている。データ処理装置100は、非暗号プログラム読込手段101と、暗号鍵算出手段102と、暗号化プログラム読込手段103と、暗号解除手段104を含む。ファイル装置110は、非暗号プログラム記憶手段111と暗号化プログラム記憶手段112を含む。

【0010】これらの手段はそれぞれ概略つぎのように動作する。

【0011】非暗号プログラム記憶手段111には暗号化されていないプログラムコードが格納されている。暗号化プログラム記憶手段112には暗号化されたプログラムコードが複数のブロック1、2、 \dots n に分割されて格納されている。これらは、非暗号プログラム記憶手段111に格納された暗号化されていないプログラムコード、暗号化されたブロック1、2、 \dots n の順に、データ処理装置100に読み込まれるものとする。

【0012】非暗号プログラム読込手段101は、非暗号プログラム記憶手段111から、図示していない主記憶上に、暗号化されていないプログラムコードを読み込む。

【0013】暗号鍵算出手段102は、この主記憶上に

あるプログラムコードの一方関数（ハッシュ関数など）を使用して、読み込まれる暗号化されたプログラムコードブロックを平文化するための暗号鍵を生成する。暗号化プログラム読込手段103は、暗号化プログラム記憶手段112から主記憶上に次に実行する暗号化されたプログラムコードを読み込む。暗号解除手段104は、暗号鍵算出手段102が算出した暗号鍵を使用して、暗号化されたプログラムコードの暗号を解除する。

【0014】まず、図4を参照して、ファイル装置110に書き込まれるデータを作成する暗号化装置につき、説明する。図4は、ファイル装置110に書き込まれるデータを作成するための暗号化装置の構成を示すブロック図である。

【0015】ファイル装置に格納されるべき、プログラムコードは、分岐回路201に供給される。分岐回路は、供給されたプログラムコードを、 $(n+1)$ 個のブロックに分割し、最初のブロックを図1の非暗号プログラム記憶手段111に書き込むとともに、暗号鍵算出手段102に供給する。また分岐回路は、最初のブロックを出力後、最初のブロック（第0番目のブロック）を除く n 個のブロックを順に、遅延回路203及び暗号鍵算出手段102に出力する。

【0016】暗号鍵算出手段は、分岐回路201から最初のブロックが供給されると、この最初のブロックのプログラムコードからハッシュ関数等の一方関数を用いて、最初のブロックの次のブロック（第1番目のブロック）のデータを暗号化するための第1の暗号鍵を算出する。この第1の暗号鍵の出力が終了すると、この暗号鍵算出手段102には、第1番目のブロック、第2番目のブロック、 \dots 第 n 番目のブロックが順次供給され、同様に、第2の暗号鍵、 \dots 第 n の暗号鍵が、順次出力され暗号化器204に供給される。

【0017】一方、遅延回路203は、分岐回路から順次供給される第1番目から第 n 番目のブロックは、遅延回路に203により、1ブロック分遅延されて暗号化器に供給される。この結果、第1のブロックは、第0のブロックのデータにより生成された第1の暗号鍵により暗号化され、図1の暗号化プログラム記憶手段112に格納される。第2のブロックは、第1のブロックのデータにより生成された第2の暗号鍵により暗号化され、図1の暗号化プログラム記憶手段112に格納される。以下同様に、第 i 番目のブロックは、第 $(i-1)$ 番目のブロックのデータにより生成された第 i の暗号鍵により暗号化され、図1の暗号化プログラム記憶手段112に格納される。

【0018】このようにして、図1の非暗号プログラム記憶手段111には暗号化されていないプログラムコードが格納され、暗号化プログラム記憶手段112には暗号化されたプログラムコードが複数のブロック1、2、 \dots n に分割されて格納される。

【0019】次に、図2のフローチャートを参照して本実施形態の全体の動作について詳細に説明する。

【0020】暗号化プログラム記憶手段112には、非暗号化プログラム記憶手段111内に格納されたプログラムコードに後続するプログラムコードが複数のブロックに分割されて格納されている。暗号化プログラム記憶手段112には、それぞれのブロックのプログラムコードは、一つ前のブロックのプログラムコードのハッシュ値を暗号鍵に使用して暗号化され、格納されている。

【0021】まず、ステップA1では、非暗号プログラム読込手段101は、非暗号プログラム記憶手段111から暗号化されていないプログラムコードを主記憶上に読み込み、プログラムコードの実行を開始する。この処理は通常、オペレーティングシステムのプログラム実行機構で管理されている。

【0022】次に、ステップA2では、暗号鍵算出手段102は、非暗号プログラム読込手段101が主記憶上に読み込んだプログラムコードをハッシュ関数などの一方関数で変換し、暗号鍵を生成する。

【0023】ステップA3では、暗号化プログラム読込手段103は、暗号化プログラム記憶手段112から主記憶上に次に実行する暗号化されたプログラムコードを読み込む。

【0024】ステップA4では、暗号解除手段104は、暗号鍵算出手段102が算出した暗号鍵を使用して、暗号化されたプログラムコードの暗号を解除する。

【0025】ステップA5では、暗号鍵算出手段102は、暗号解除されたプログラムコードのハッシュ値を算出し、これを次の暗号解除時の暗号鍵とする。

【0026】次に、ステップA6では、現在主記憶上にある暗号解除されたプログラムコードを実行する。この処理の中で、不正コピーの判定等を行う。

【0027】ステップA7では、暗号化プログラム記憶手段112内の全てのブロックのプログラムコードにつき、ステップA3からA6までの処理が行われたか否かが判定され、全てのブロックのプログラムコードについて処理が実行されていない場合には、データ処理装置の動作は、ステップA3に戻る。

【0028】図3は不正利用者によるプログラムコードの改竄の試みが行われなかった場合の動作を現す説明図である。プログラムコードの改竄が行われなかった場合には、暗号化されたプログラムコードを暗号解除するための暗号鍵a、b、cは正しい値が得られる。

【0029】非暗号化プログラム記憶手段111に格納されている暗号化されていないプログラムコード1を改竄した場合、ステップA2で算出される暗号鍵は、本来の暗号鍵aと全く異なった物となる。このため、ステップA4で暗号解除されたプログラムコード2は本来のプログラムコードと全く異なったコードとなり、以降のプログラムは正常に動作しなくなる。暗号化プログラム記

憶手段112内のプログラムコードが改竄された場合にも、改竄されたブロックより後のブロックのプログラムコードは、ステップA4で暗号解除されても、本来のプログラムコードと全く異なったコードとなり、以降のプログラムは正常に動作しなくなる。

【0030】このようにプログラムコードを一個所改竄すると、以降のプログラムを正常に動作させるためには、全てのブロックの暗号鍵を何らかの手段で取得し、暗号解除手段104が使用する暗号鍵として使用するよう改竄する必要がある。このような不正利用者にとって好ましい改竄は、ブロックの数を増やすほど困難になる。

【0031】この実施形態では、改竄検出の対象をプログラムコードとしたが、暗号鍵の生成時にデータ領域の一方関数を使用することによって、データの改竄を検出することも可能である。この場合には、上述の説明において、「プログラム」を、「データ」と読み替えれば良い。

【0032】また、以上説明した実施形態では、非暗号プログラム記憶手段111内のプログラムコードあるいはデータは、暗号化されずに平文にままで格納されているものとして説明していたが、この非暗号プログラム記憶手段111内のプログラムコードあるいはデータは、前もって定められた暗号鍵により、暗号化されていても良いことは明かであろう。この場合には、図1の非暗号プログラム読み込み手段101は、この前もって定められた暗号鍵に基づいて、記憶手段111内のデータを暗号解除して出力する機能を併せて有する。

【0033】

【発明の効果】本発明では、プログラムコードの大部分が暗号化されているため、逆アセンブラツールなどの解析ツールでプログラムコードを解析すること自体が困難である。また、本発明では、暗号鍵算出手段102が現在実行しているプログラムコードの一方関数を暗号解除鍵として算出し、次に実行するプログラムコードの暗号解除に使用しているため、プログラムコードを改竄して不正利用することが困難である。

【図面の簡単な説明】

【図1】本発明の一実施形態を示すブロック図である。

【図2】本発明の一実施形態の動作を説明するためのフローチャートである。

【図3】不正利用者によるプログラムコードの改竄の試みが行われなかった場合の動作を現す説明図である。

【図4】本発明のファイル装置に書き込まれるデータを作成するための暗号化装置の構成を示すブロック図である。

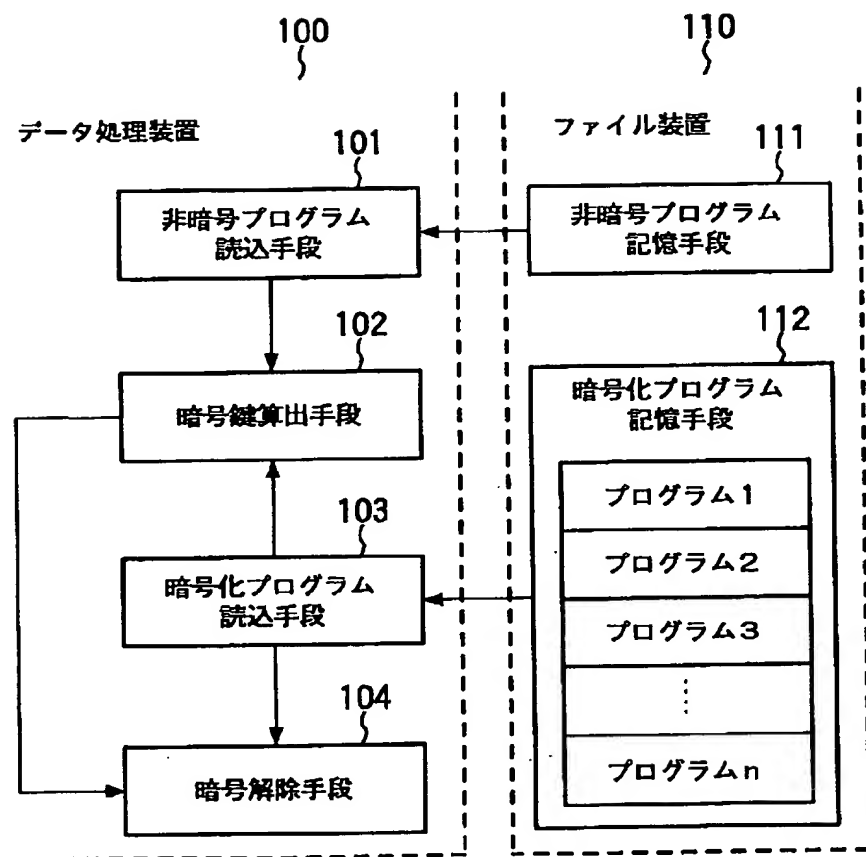
【符号の説明】

- 100 データ処理装置
- 101 非暗号プログラム読込手段
- 102 暗号鍵算出手段

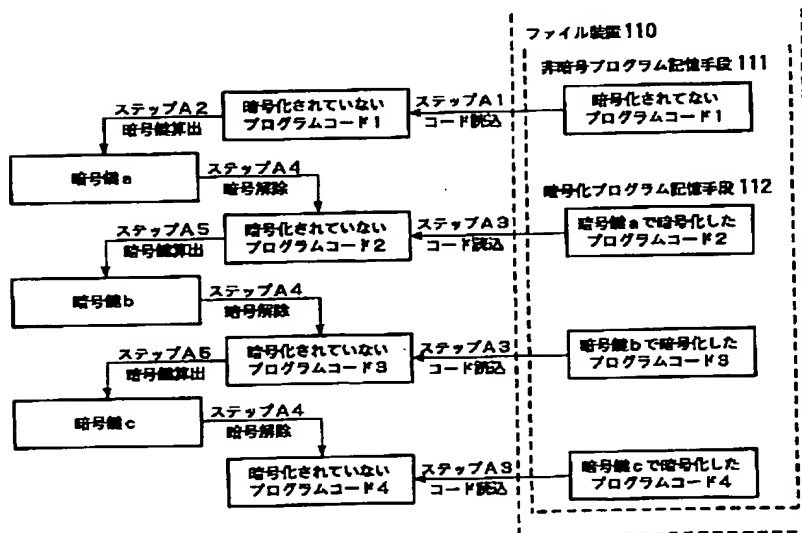
103 暗号化プログラム読込手段
 104 暗号解除手段
 110 ファイル装置
 111 非暗号プログラム記憶手段

112 暗号化プログラム記憶手段
 201 分岐回路
 203 遅延回路
 204 暗号化器

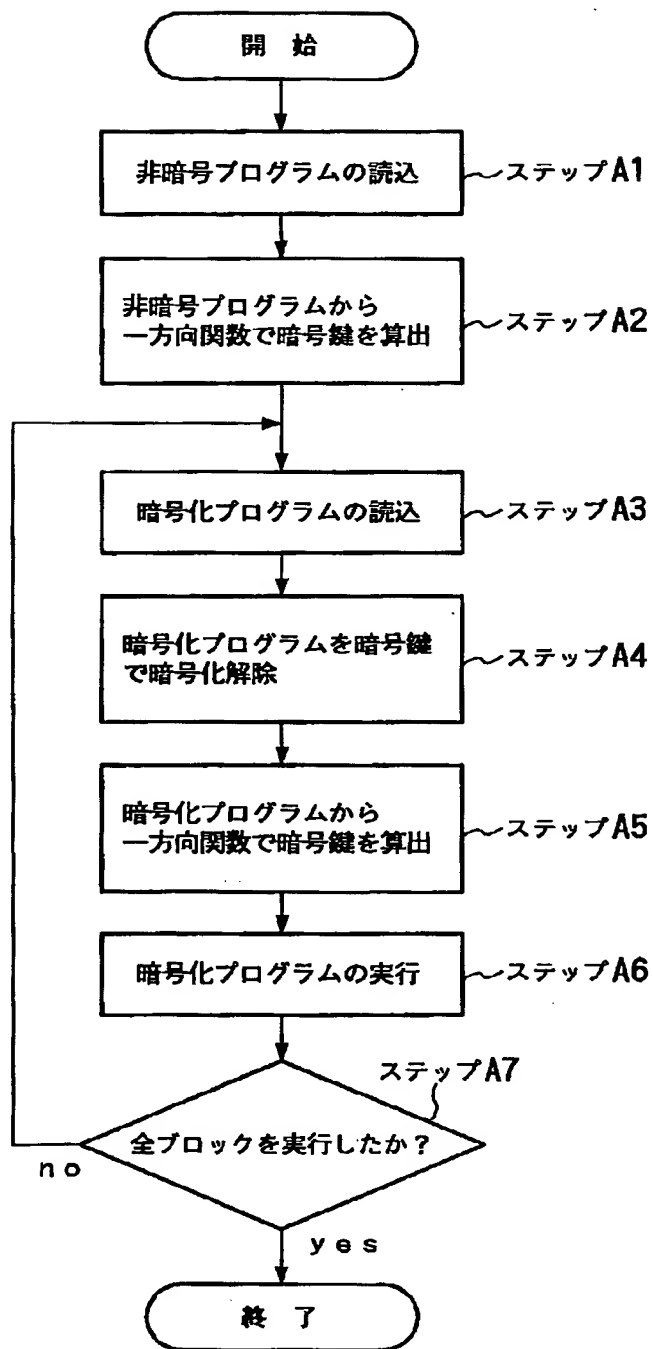
【図1】



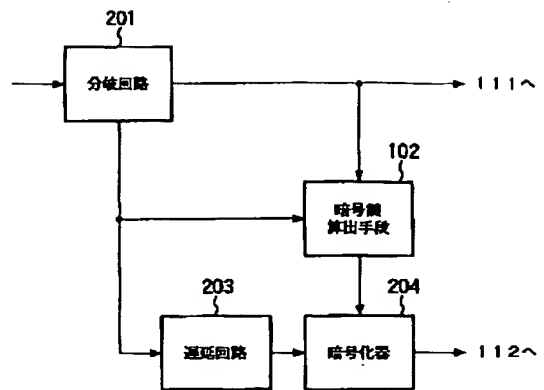
【図3】



【図 2】



【図 4】



BEST AVAILABLE COPY